REMARKS

Claims 1, 2, and 4 are amended. Claims 6-20 are canceled without prejudice or disclaimer. No new matter is added by these amendments. Claims 1-5 are pending. By amending and canceling the claims, applicant is not conceding that the claims are non-statutory under 35 U.S.C. 101, 102, 103, and 112 and is not conceding that the claims are unpatentable over the art cited by the Office Action, as the claim amendments and cancellations are only for the purpose of facilitating expeditious prosecution. Applicant respectfully reserves the right to pursue these and other claims in one or more continuation and/or divisional applications. Applicant respectfully requests reconsideration and allowance of all claims in view of the amendments above and the remarks that follow.

35 U.S.C. 112 Rejections

Claims 1-20 are rejected under 35 U.S.C. 112 because "a first password" "is subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the invention," and the Office Action argues "Apparently, there is only one password disclosed in the original disclosure."

Applicant respectfully traverses these grounds for rejection for the reasons argued below.

First, the claims as originally filed recited two passwords: Originally filed claim 1 recited "a password" while originally file claim 5 recited "a second password," so multiple passwords were recited in the originally filed claims, which are part of the original disclosure, as specified by MPEP 608.04: "In establishing a disclosure, applicant may rely not only on the specification and drawing as filed but also on the original claims if their content justifies it."

Second, Fig. 6A shows two "do" loops, the first starting at block 610 and the second starting at block 630, each of which is executed once "for each password in form," which describes multiple passwords.

Third, Fig. 3A illustrates a password list 172, having multiple records 305 and 310, one for each password, which describes multiple passwords.

Fourth, applicant's specification at page 13, line 28 and page 14, lines 1-7 recites: "If the determination at block 605 is true, then the form does contain a password, so control continues from block 605 to block 610 where the controller 170 performs a loop for each password in the form. So long as there remain unprocessed passwords in the form, control continues from the beginning of the loop at block 610 to block 615. After all of the passwords in the form have been processed, the loop exits from block 610, and control continues from block 610 to block 630. Thus, for each password in the form, control continues from block 610 to block 615 where the controller 170 computes a key based on the password," which describes multiple passwords.

Finally, applicant's specification at page 15, lines 19-27 recites: "When the loop at block 610 completes, control continues from block 610 to block 630 where the controller 170 performs a loop for each password in the form. So long as a password in the form remains unprocessed, control continues in the loop from block 630 to block 635 where the controller 170 writes an entry to the password list 172 if the password is not already in the password list 172. Control then returns from block 635 to block 630, as previously described above. Once the loop that starts at block 630 completes, and each password in the form has been processed, then control continues from block 630 to block 640 where the controller 170 submits the form via the network 130," which describes multiple passwords.

Claims 1-20 are rejected under 35 U.S.C. 112 because "the examiner finds no support in the original disclosure about 'wherein the first password is allowed to be submitted to the set of pages.'" Applicant respectfully traverses these grounds for rejection for the reasons argued below.

Page 13, lines 3-6 of applicant's specification recites: "A form is a construct that facilitates the sending of information from the user of the page 176 back to the server 160 that originated the page. One type of information that the user of the page 176 can send to the server 160 via a form is a password."

Fig. 6B illustrates block 670, which recites: "deny form submission" while Fig. 6A illustrates block 640, which recites "submit form," and the logic of block 640 is executed after the processing of each password in the form is done, as illustrated by blocks 630 and 635. Thus, block 640 in Fig. 6A is an example of allowing submission of passwords to pages, and block 670 in Fig. 6B is an example of denying submission of passwords to pages.

The execution of the logic illustrated by blocks 640 and 670 is conditional upon the determinations made by the logic illustrated by blocks 660 and 665 of Fig 6B. If the determination made by the logic of block 665 is true for the passwords in the form, then block 640 will be executed, which allows submission of the passwords to the pages. Using the example illustrated in the specification, the determination made by the logic of block 665 is true if the URLs in the entry for the passwords match the URL in the entry of the current page that was loaded (explained at page 14, lines 16-28 and at page 5, lines 1-13). Thus, if the URLs in the entry associated with the passwords in the form match the URL in the entry associated with the page that was loaded, the form is allowed to be submitted to the pages.

Thus, applicant's specification supports "the first password is allowed to be submitted to the server that originated the set of pages," as recited in claim 1.

Claims 1-20 are rejected under 35 U.S.C. 112 because "if the first password is allowed to be submitted to the set of pages, then why it is necessary to determine whether a first password is restricted to a set of page?"

Claim 1 is amended to recite: "if the first password is restricted to the set of pages, denying submission of the first password outside the set of pages, wherein the first password is allowed to be submitted to the server that originated the set of pages; and if

the first password is not restricted to the set of pages, allowing submission of the password outside the set of pages," which clarifies the relationship of restriction and submission.

Claims 2-5 are statutory under 35 U.S.C. 112 for depending on claim 1. Claims 6-20 are canceled without prejudice or disclaimer, so the rejections are moot.

35 U.S.C. 101 Rejections

Claims 11-15 are rejected under 35 U.S.C. 101. Claims 11-15 are canceled without prejudice or disclaimer, so the rejection is moot.

35 U.S.C. 102 and 103 Rejections

Claims 1-3, 6-8, 11-13, and 16-18 are rejected under 35 U.S.C. 102(b) over Child (U.S. Patent 6,341,352). Claims 4-5, 9-10, 14-15, and 19-20 are rejected under 35 U.S.C. 103(a) over Child. Applicant respectfully submits that the claims are patentable over the Child because all of the elements of the claims are not taught or suggested by Child, for the reasons argued below.

Claim 1 recites: "determining whether a first password is restricted to a set of pages, wherein the determining further comprises in response to each of the pages in the set being retrieved from a server, determining whether at least one of the pages in the set comprises password restriction control information that specifics an address of a domain and restriction of password use to within the domain; if the first password is restricted to the set of pages, denying submission of the first password outside the set of pages, wherein the first password is allowed to be submitted to the server that originated the set of pages; and if the first password is not restricted to the set of pages, allowing submission of the password outside the set of pages."

In contrast to claim 1, the Child expired password is not allowed to be submitted anywhere because, as described in Child at column 6, lines 47-49, "At step 80, the

routine redirects the user to a security subprogram that is used to modify, alter or otherwise change the password," instead of completing the transaction, as described in Child at column 6, lines 41-44. Thus, Child teaches away from claim 1 because Child disallows all submission of an expired password while claim 1 conditionally allows and conditionally disallows submission of the first password depending on whether the first password is restricted to the set of pages.

In further contrast to claim 1, Child (at Fig. 4, block 74 and column 6, lines 36-38) determines whether a password is expired by invoking a "PathCheck" function that "checks with the session manger to determine whether the user has appropriate DCE credentials." A "PathCheck" function and "check[ing] with the session manger" are unrelated to a page that comprises password restriction control information because at the time Child performs its password expiration checking, the Child document has not yet been retrieved, as explained by Child at column 6, lines 44-50 and 65-67, which is illustrated in Fig. 4, blocks 88 and 90 that retrieve the document, which occur subsequent to blocks 74, 78, and 80 that perform the expired password processing.

Thus, Child does not teach or suggest "in response to each of the pages in the set being retrieved from a server, determining whether at least one of the pages in the set comprises password restriction control information that specifics an address of a domain and restriction of password use within the domain," as recited in claim 1 because Child's expired password processing occurs prior to the Child document being retrieved. In contrast, the "determining" of claim 1 occurs after the page has been retrieved because the "determining" is performed "in response to each of the pages in the set being retrieved."

Claims 2-5 are dependent on claim 1 and are patentable for the reasons argued above, plus the elements in the claims. Claims 6-20 are canceled without prejudice or disclaimer, so the rejections are moot.

Conclusion

Applicant respectfully submits that the claims are in condition for allowance and notification to that effect is requested. The Examiner is invited to telephone Applicant's attorney (651-645-7135) to facilitate prosecution of this application.

If necessary, please charge any additional fees or credit overpayment to Deposit Account No. 09-0465.

Respectfully submitted,

Date: February 8, 2008

Owen J. Gamon
Reg. No. 36,143
(651) 645-7135

IBM Corporation
Intellectual Property Law
Dept. 917, Bldg. 006-1
3605 Highway 52 North
Rochester, MN 55901

CERTIFICATE UNDER 37 CFR 1.8: I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop RCE, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, or is being transmitted via facsimile to the Commissioner for Patents, 571-273-8300, on February 8, 2008.

Owen J. Gamon
Name

Signature